Overview of the mobility related security challenges in LPWANs

H. Jradi, A.E. Samhat, F. Nouvel, M. Mroue, Jean-Christophe Prévotet

Overview of the Mobility Related Security Challenges in LPWANs

Hassan Jradi[1,2], Abed Ellatif Samhat[1], Fabienne Nouvel[2], Mohamad Mroue[1], and Jean-Christophe Prévotet[2]

[1]Lebanese University — Scientific Research Center in Engineering, Hadath, Lebanon.
[2]Institut National des Sciences Appliquées de Rennes — IETR, Rennes, France.
[1]Email: samhat@ul.edu.lb, mohamad.mroue@ul.edu.lb
[2]Email: firstname.lastname@insa-rennes.fr

Abstract

The Internet of Things (IoT) is a new emerging system of interconnected devices that experiences significant growth in a wide variety of applications. The rising communication technologies for IoT are the Low Power Wide Area Networks (LPWANs) having long range, low cost and low power characteristics. In this context, an important part of the applications requires the mobility of the end devices with secure communications. In this paper, we consider the mobility management solutions in LPWAN networks and we investigate how they ensure security. We first review the basic IoT security requirements and the typical IoT protocol stack. We then focus on the existing mobility management solutions in LPWAN and we highlight the mobility related security issues by checking the attacks that can be performed in case of mobility. Furthermore, we evaluate the security in each mobility solution by checking the aforementioned attacks and we draw a comparison study.

Index terms*— *Internet of Things, LPWAN, Mobility, Security.

1 Introduction

The Internet of Things (IoT) refers to the huge number of devices connected to the internet for various purposes including data collection, information sharing, smart system control, etc. The prominent requirements for IoT communication with the end user are the low power consumption, the long range of communication, and the cost efficiency. Low-Rate Wireless Personal Area Network (LR-WPAN) technologies such as ZigBee and Bluetooth do not fit long range communication requirements but their cost and energy consumption are relatively low. Other technologies based on common cellular networks as 2G, 3G, and 4G have high power consumption but can span long communication ranges. The lack of a technology satisfying all the IoT communication requirements led to the development of a new type of wireless communication technology called Low Power Wide Area Network (LPWAN). The long range, low cost and low power characteristics of LPWAN [1, 2] give it an increasing prevalence in the research and manufacturing areas [3]. Among the various LPWAN technologies, the most popular today are LoRaWAN [4], NB-IoT [5], SigFox [6] and DASH7 [7, 8].

In recent years, IoT is experiencing significant growth in a wide variety of applications including healthcare, supply chain, smart cities, smart vehicles,

etc. An important part of such applications requires the mobility of the end devices that are frequently moving and changing their locations. Therefore, a suitable mobility management process should be employed to provide a roaming feature for devices when moving away from their home networks. Many solutions are proposed in the literature for mobility management in the Internet, and several of them propose the use of a network layer protocol like Mobile IPv6 (MIPv6) [9], Fast Handover MIPv6 (FMIPv6) [10], Network Mobility (NEMO) [11], Proxy Mobile IPv6 (PMIPv6) [12], etc. Other solutions are designed particularly for LPWAN technologies that come with restrictions on many parameters like the maximum payload length and the number of messages sent during a time interval. For example, the maximum payload length is 243 bytes for LoRaWAN frame, 1600 bytes for NB-IoT, while the daily message number is restricted to 140 messages per day in uplink and 4 messages in downlink for Sigfox [13].

In addition to mobility needs, IoT applications should consider the requirements related to security. Any solution or communication technology used to establish a communication between an IoT device and an end user should take the basic security requirements as main requirements in the solution plan or in the communication scheme, which include the authenticity, confidentiality, integrity, and availability, in addition to some specific requirements to IoT related to resource limitations such as short battery lifetime and small memory size. The security issues can be classified according to several categories, like impact severity, consequences, device or network related, used protocol stack, etc. Moreover, mobile IoT rises new types of security issues related to device mobility itself, and from the management process responsible for the handle of the mobility process.

Several papers presented an overview of the security in IoT such as [14], [15] and [16]. The focus in these papers was mainly on common security attacks in IoT networks. But in this paper, we consider the mobility related security issues. To our knowledge, this is the first paper highlighting such mobility related security issues.

The rest of the paper is organized as follows. In Section 2, we present a typical IP-based protocol stack for IoT and the security requirements. Next in Section 3, we summarize the architectures of the most famous LPWAN technologies which are LoRaWAN and NB-IoT, and how each technology can achieve roaming. Further, in Section 4, we define mobility and we present the three existing solutions for mobility in LPWAN. After, in Section 5, we present the mobility related security issues. Finally, we evaluate the aforementioned mobility solutions according to the presented security issues in Section 6.

2 IoT Protocol Stack and Security Requirements

In this section, we present a typical IP-based protocol stack for IoT. Then, we briefly review the basic security requirements to achieve safe communication in an IoT environment.

2.1 IoT Protocol Stack

Figure 1 shows a typical IP-based protocol stack for IoT. This stack is very similar to TCP/IP protocol [17], but it is adapted to work in an environment with resources-constrained devices, which is the most critical constraint in an IoT environment. Similar to TCP/IP protocol, this stack consists of the five prevailing layers: application, transport, network, link and physical; in addition to the adaptation layer.

At the application layer, two main protocols are used: the Constrained Application Protocol (CoAP) and the Message Queuing Telemetry Transport (MQTT). CoAP is used as a web communication protocol adopted by nodes and networks having limited resources. CoAP is based on request/response model between nodes and designed to be easily integrated into the Web [18]. CoAP uses the User Datagram Protocol (UDP) at the transport layer and a simple mechanism for re-transmission in case of packet loss [19]. MQTT is based on publish/subscribe model and on the Transmission Control Protocol (TCP). MQTT is designed to work in low bandwidth wireless environments allowing at the same time many to many communication and

can support Secure Sockets Layer (SSL) and Transport Layer Security (TLS) [20]. Other application layer protocols also exist for IoT such as the Extensible Messaging and Presence Protocol (XMPP) [21], RESTful [22], and the Advanced Message Queuing Protocol (AMQP) [23].

As mentioned, UDP is used at the transport layer for CoAP. Although a reliable protocol is required at this layer, the TCP is less used for many reasons. First, in many IoT technologies, IoT devices are scheduled to go into sleep mode regularly or after transmission, and a long term connection cannot be held. Second, TCP adds a considerable overhead compared to the length of data sent by an IoT device. Third, many applications using the data sent by IoT devices require low latency. Also, the overhead added by the TCP adds a delay of transmission which is not suitable for such applications [24]. For all these reasons and since UDP does not have the mentioned problems, UDP was preferred over TCP at the transport layer.

Many key features motivate to use IPv6 at the network layer. IPv6 can achieve high scalability especially when comparing it to IPv4. Scalability comes essentially from the number of addresses that can be assigned in the network. IPv6 has 128-bit for the address space whereas IPv4 has only 32-bit which is almost occupied by the traditional computer networks. Another feature supported by IPv6 is the Stateless Address Auto-Configuration (SLAAC) which helps in getting addresses without the need for processes like Dynamic Host Configuration Protocol (DCHP) used in IPv4. An important feature in IPv6 is the optimized mobility support that avoids triangular routing, provided by using the IPv6 extension headers [25].

One of the main challenges of deploying IPv6 in IoT is the large size of IPv6 headers, therefore, an adaption layer is usually employed. The main purpose of the adaptation layer is to compress IPv6 headers which reduces the packet length and thus the power needed for transmission. In addition, adaptation layer is used in packet fragmentation mechanism in networks that have small maximum transmission unit length. A well known adaption layer protocol is IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) [26], others exist such as RObust Header Compression (ROHC) [27] and Static Context Header Compression (SCHC) [28].

The two lower layers, physical and link layers, consist of the technology used and supported by the IoT device, it can belong to Low Rate Wireless Personal Area Networks (LR-WPANs) like Zigbee and Bluetooth, or Low Power Wide Area Networks (LPWANs) like LoRaWAN and NB-IoT, or other types of link layer technologies. An IoT device can support more than one technology at the same time which helps in mobility when moving between networks employing different link layer technologies.

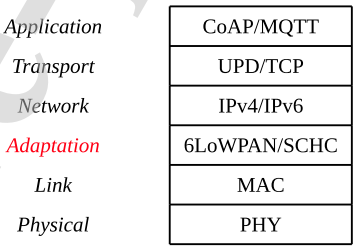


Figure 1: IoT Protocol Stack.

2.2 IoT Security Requirements

The IoT networks inherit the common network security requirements, which are **C**onfidentiality, **I**ntegrity and **A**vailability, widely known as the **CIA** triad [29], added to the authenticity.

- **Confidentiality (C):** refers to the prevention of data exposure to unauthorized parties. Since the data sent by IoT devices could pass through insecure paths before arriving at the destination, an appropriate mechanism should be employed to prevent an eavesdropper from revealing them.

- **Integrity (I):** the data should be exchanged and stored in a manner that prevents any unauthorized party from altering them, which can lead to faulty decisions, or manipulating them for other malicious purposes.

- **Availability (Av):** the service provided by the IoT network should be reachable anytime, thus, all the nodes forming the network should be protected from attacks that hinder the provision of services like Denial of Service and Jamming attacks.
- **Authenticity (Au):** refers to the ability of nodes constituting the network to identify each other. The identities of the nodes participating in a session should be verified when establishing it and until terminated. An attacker succeeding to break the authentication mechanism can hijack the session, spoof the identities and violate the privacy of users.

Here we present the security requirements in order to evaluate the mobility related security issues shown in section 5 and the mobility solutions shown in section 6 according to these requirements.

3 Low Power Wide Area Network (LPWAN)

We describe in this section the typical architectures of LPWAN technologies. Although the diversity of LPWAN technologies, the most prominent today are LoRaWAN, NB-IoT and Sigfox [3]. In the following, the focus will be on LoRaWAN as a typical example of unlicensed LPWAN technology and NB-IoT as a typical example of licensed LPWAN technology. We then highlight the roaming within such technologies.

3.1 LoRaWAN

3.1.1 Architecture

LoRaWAN is a communication technology specified by LoRa Alliance [30] designed to provide long range communication for resource-constrained devices. A roaming feature is added to the last version of LoRaWAN (version 1.1) [31]. The focus will be on this version whose architecture is illustrated in figure 2.

- End Device (ED): is usually a sensor node like a humidity sensor, a temperature sensor, a health monitoring device, etc. The end device sends the captured data as an uplink message to the network via the gateways [32].
- Network Server: is the intelligent part of the network, the main tasks are the routing of the end device messages to the application server, the treatment of the messages received from several gateways and the choice of the best gateway for the downlink message path [33]. There are 3 types of network server:
  - Home Network Server: is the network server to which the end device initially belongs to.
  - Serving Network Server: involved in case of active roaming.
  - Forwarding Network Server: involved in case of passive roaming.
- Join Server: responsible for the join procedure and the generation of encryption keys in case of over the air activation (OTAA).
- Gateway: acts as a relay between the end device and the network server. The gateway receives and forwards the messages in both directions (uplink and downlink) without any intervention. Usually, the uplink messages (from the end device to the network server) are duplicated at the network server since each message can be received from more than one gateway and each message arriving at the gateway is sent to the network server. The downlink messages (from the network server to the end device) are unique since the network server chooses the best downlink path, i.e. gateway with the best link conditions. The communication between the end devices and the gateways is based on LoRa physical layer, whereas the communication between the gateway and the network server is based on IP protocol [34].
- Application Server: receives messages from the network server in order to perform the required analysis and make decisions. The application server can also be a cloud where end users access and view the messages.

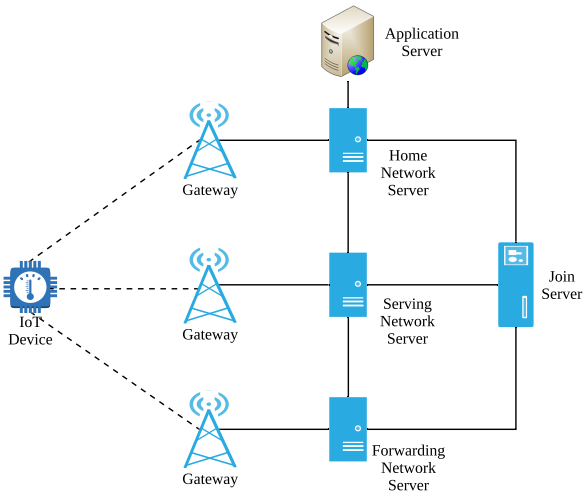


Figure 2: LoRaWAN Architecture.

3.1.2 Roaming

Roaming is the ability of an end device to send and receive data even though it is outside the coverage of its home network by the means of the visited network where an agreement should be ratified between the two networks [35].

LoRaWAN supports two distinct types of roaming. The first one is called **passive roaming** where the end device after leaving the coverage of its home network can hold its connection via the forwarding network server which only transmits the packets from the end device to its home network server and vice versa. But the end device management (such as the link layer identity, network session key) is still under home network server control, hence the name of the forwarding network server. The second one is called **active roaming** or "handover" where the difference here is that the serving network server handles the end device management. The end device data still passes through the home network server which forwards them in its turn towards the application server.

3.2 NB-IoT

3.2.1 Architecture

NB-IoT is a network protocol standardized in Release 13 by the 3rd Generation Partnership Project (3GPP) in June 2016. It is developed to work along with cellular networks like LTE (Long-Term Evolution) and GSM (Global System for Mobile Communications) under licensed frequency bands [36]. Since NB-IoT is integrated into the cellular network, it inherits the common cellular network architecture with slight modifications as shown in figure 3. According to the standard [37], an end device is attached to the network by two means:

- With Packet Data Network connection (PDN): a connection with the PDN is required to complete the attach procedure. IP data packets pass through the packet data network gateway (PGW) while Non-IP data packets pass through the Service Capability Exposure Function (SCEF).
- Without Packet Data Network connection: which is a new feature introduced in Release 13 allowing end devices to remain attached to the network without a PDN connection. The connection is based on the control plane established between the end device and the mobility management entity (MME) of the core network. This is effective where a large number of devices rarely transmitting data would maintain a long-life connection, thus the end device is connected with short message service (SMS) only to transmit data.

3.2.2 Roaming

NB-IoT benefits from the LTE functionalities supporting roaming in two ways. The first one is through the routing from the serving gateway (SGW) of the visited network to the PGW of the home network, the traffic sent by the end device still passes through the home network. The second one is by the rupture between the home network and the visited network where the traffic passes through the PGW of the visited network [38]. An end device can also benefit the control plane based connection to suspend and

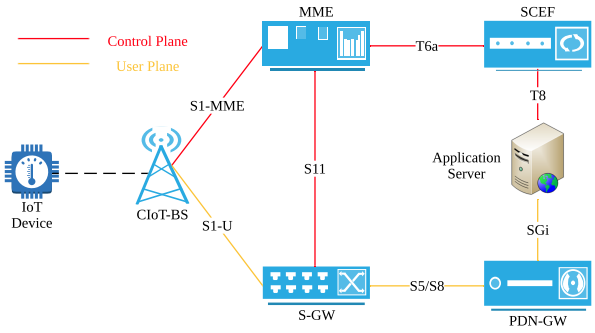


Figure 3: NB-IoT Network Architecture.

resume the connection and send data whenever it is under a Cellure IoT Base Station (CIoT-BS) coverage [39].

Next, we will show how roaming is optimized in LPWAN by proposing new solutions to manage mobility.

4 Mobility Solutions for LPWANs

This section highlights the different types of mobility in IoT networks, and more especially in LPWANs. Furthermore, we consider the only three solutions for mobility management in LPWAN existing in the literature.

4.1 Mobility in LPWAN

Mobility is the ability of a moving end device to be always accessible to other correspondent nodes when changing the gateway used to reach the network [40]. Moreover, mobility can be seen as the re-establishment process of the connection during end device movement between two network operators, whether or not having different access technologies. In several case, connection continuity must be ensured when the end device changes its gateway and, therefore, it must always be able to send/receive data via the new gateway to/from the correspondent node without interrupting the connection. There are 4 types of mobility as summarized in table 1.

In the following, we consider an end device with a full protocol stack as shown in section 2. For LoRaWAN technology, it is known as a link layer technology. Adding a network layer for LoRaWAN devices can be achieved in several ways as discussed by [27]. Ayoub *et al.* in [27] also discussed how to add a network layer for several existing LPWAN technologies.

The first type is the simplest, where the end device moves from the coverage of a gateway to another using the same technology and belongs to the same network operator as shown in figure 4(A), we call this type of mobility "Homogeneous Intra-domain mobility". From a technical point of view, such type of mobility may lead to a change in the link layer identity, for example, a passive roaming in LoRaWAN does not lead to a change in the link layer identity while an active roaming leads to a change in the link layer identity. Regarding the network layer identity (IPv4, IPv6, etc..), it may change or not according to the new network layer point of attachment of the new gateway in the core network. In this type of mobility, the mobility management process is simple since it should take care of neither the different technologies management nor the registration mechanism with another network operator. Usually, this type of mobility is handled by the technology itself as in LoRaWAN and NB-IoT.

In the second type, the end device moves from the coverage of a gateway belonging to a network operator, called the home network operator, to another belonging to a different network operator, called visited network operator, using the same technology as shown in figure 4(B), we call this type of mobility "Homogeneous Inter-domain mobility". A change in the network operator means a necessary change in the network layer point of attachment leading to a change in the network layer identity, the link layer is also changed as a new link layer access point used to attach in the visited network. In this case, the mobility management process should take into consideration the registration and the authentication mechanism when the end device moves between different networks. This type of mobility is already built in

Type	Technology	Operator	Link Layer ID	Network Layer ID
Homogeneous Intra-domain	Same	Same	May change	May change
Homogeneous Inter-domain	Same	Different	Change	Change
Heterogeneous Intra-domain	Different	Same	Change	May change
Heterogeneous Inter-domain	Different	Different	Change	Change

Table 1: Types of mobility

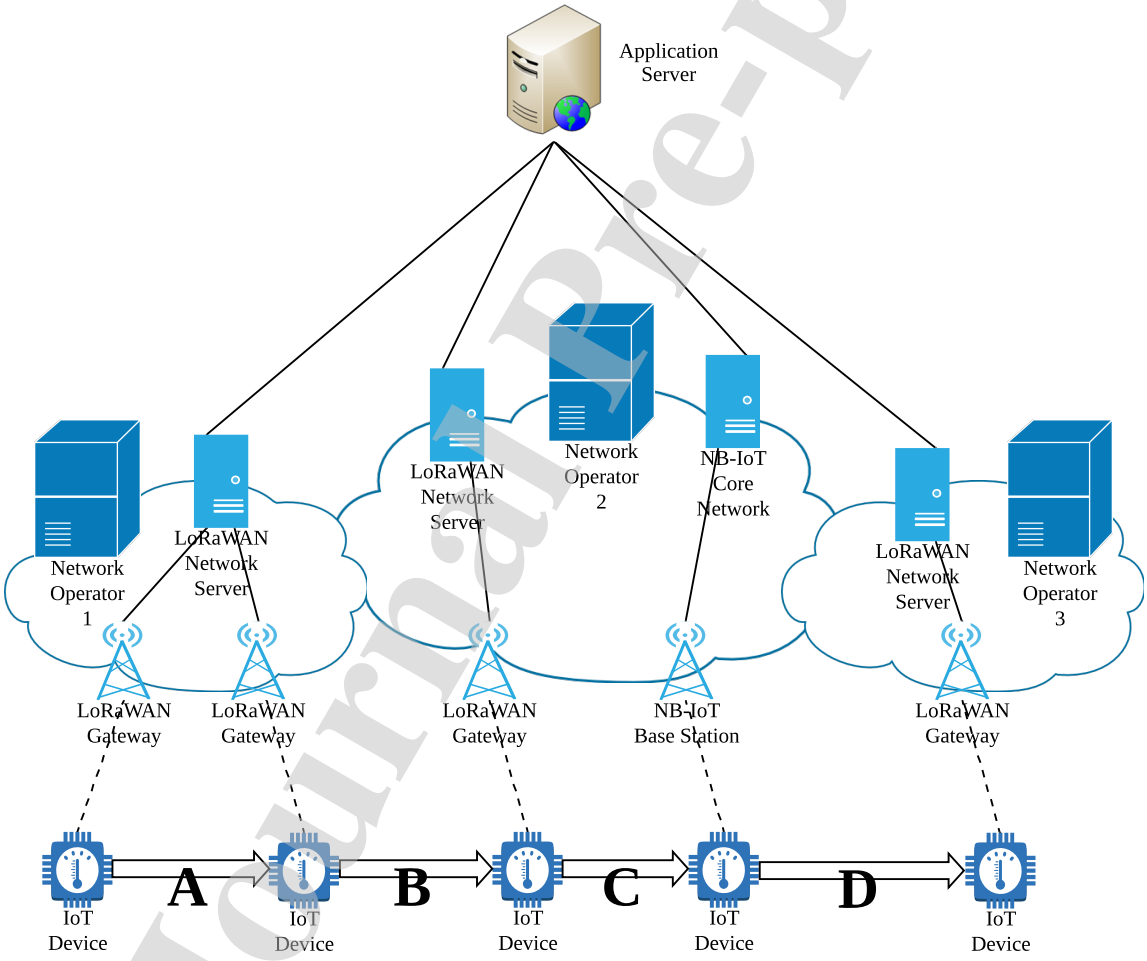


Figure 4: End device moving between different gateways and achieving different types of mobility.

LoRaWAN v1.1 and in NB-IoT as shown in section 3.

The third type is a little bit complex, where the end device moves from the coverage of a gateway to another using different technology and belonging to the same network operator as shown in figure 4(C), we call this type of mobility "Heterogeneous Intra-domain mobility". A compulsory condition is that the end device should implement the two technologies. Thus, the mobility management process should take into account how to switch between different technologies. A change in the technology leads to a necessary change in the link layer identity, while for the network layer identity, as in the first type of mobility, it may change or not according to the new network layer point of attachment in the core network.

The fourth type is the combination of the second and the third types, which is the most complex as shown in figure 4(D). The mobility management process should manage the registration when the end device moves to the visited network and the switch between two different technologies. In this case, the link layer and the network layer identities are changed, and the new identifiers are obtained during the authentication phase with the new network operator.

Regarding the application layer identity, it is mainly managed by the application running on the application server which is often the correspondent node with whom the end device communicates. For that, this identity may or may not change according to the application requirements, and is independent of the underlying network changes.

Note that a mobility management process of type 4 is backward compatible, i.e. can handle mobility of type 3, 2 and 1. But using the process of type 4 to support mobility of lower type adds in general an overhead to the management process. For example, when using mobility management process of type 4 to manage mobility of type 2, the technology management process is not involved. Thus, according to the mobility type, the corresponding management process should be used.

Moreover, mobility always requires roaming agreements between different network operators when the mobility is of type 2 or 4, i.e. inter-domain. We define a domain as the whole network of the current operator with which the device can access the correspondent node or the application server.

Whatever the mobility type, the mobility management process must take into account the resource limitations when the end device is an IoT device. The implemented process must be aware of the increase in memory usage, battery life and the superfluity in the processing power.

4.2 LPWAN Mobility Solutions

In this section, we investigate three proposed solutions to integrate the mobility feature in LPWAN networks.

1. Blockchain based solution for roaming in LoRaWAN

This solution is proposed by Durand *et al.* [41]. The authors endeavor to achieve a decentralized architecture at the join server level and to optimize

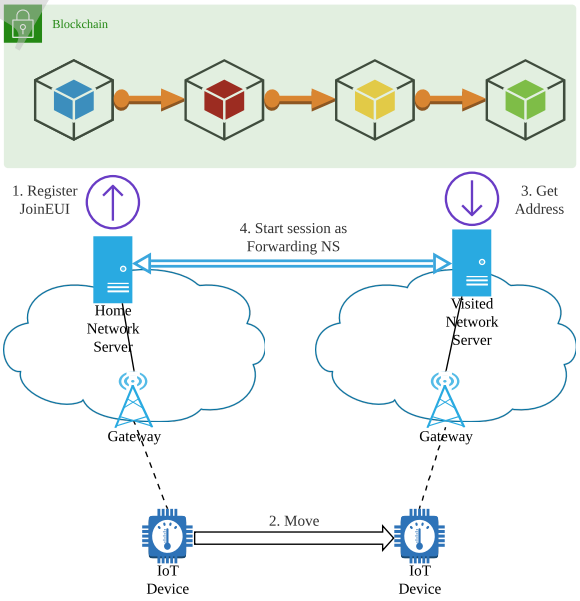


Figure 5: Blockchain based solution for roaming in LoRaWAN.

roaming in LoRaWAN v1.1, of which the homogeneous inter-domain mobility belongs.

The join procedure in LoRaWAN involves a join server to complete the process. Subsequently to an end device join request to a visited network server, which can be a forwarding or a serving network server according to the agreement, the latter sends a *home network server request* to the join server in order to recognize the home network server of this end device and start up the roaming process. The join server performs a search based on the received JoinEUI in the list of formerly registered network server addresses. Then the join server returns the corresponding home network server address to the visited network server so that it can complete the join procedure of the new end device.

Durand *et al.* propose a revised solution that replaces the join server by a blockchain smart contract as shown in figure 5. This smart contract has two main functions. The first function is *RegisterJoinEUI* which is executed by home network servers in order to register end devices under their control. This function binds the end device JoinEUI with the home network server address and appends this record to an array saved in the blockchain smart contract.

Thus, if this end device goes out of the coverage of its home network, the visited network server uses the second function, which is *GetAddress* taking a JoinEUI as an input parameter and returns the home network server address that has been mapped with this JoinEUI by the first function. For the rest of the join procedure, the home network server assigns the end device address and returns it via the forwarding network server encrypted using the application session key, and since the forwarding network server does not have information about the application session key, the authors propose to send it in an out-of-band manner.

Obviously, this solution is based on blockchain, which is a notable type of distributed ledger technologies based on a decentralized system architecture that has several advantages over centralized system architecture. Decentralized systems avoid single point of failure, since the join server which was a single server is replaced by a smart contract where the probability of the halt of the whole system at the same time due to a technical or security issue is very low. Besides, overall system performance is enhanced as join server services are distributed across nodes holding the blockchain ledger, making this solution more scalable thus supporting a higher number of end devices.

On another side, distributed systems suffer from many drawbacks. Each transaction sent to the blockchain is subject to fees, thus the transactions sent to add the mapped record between the JoinEUI with the home network server address should be paid which makes this solution less interesting to be adopted. Furthermore, many security issues exist in blockchain, because transaction validation takes some time according to the blockchain type, which is 14 seconds in Ethereum [42]. This makes the new sent data susceptible to modification or alteration attack. Adding that blockchain is susceptible to "51% attack" [43] which makes the network under attacker control if he reaches 51% of the total network computational power.

2. Distribution servers based solution for roaming in LoRaWAN

This solution is proposed by Lamberg-Liszkay *et al.* [44]. Lamberg-Liszkay *et al.* propose a decentralized architecture to achieve roaming in LoRaWAN v1.0. The authors propose the addition of a new entity called the Distribution Server. The network can still work without this server thus this solution changes nothing in LoRaWAN standard. This server works as a broker entity in LoRaWAN topology to reinforce roaming as shown in figure 6. Four services are implemented in the Distribution server to manage device roaming as described below.

- Registration Service: this service manages the registration process of a distribution server with another network or distribution server. Thus, an end device affiliated initially to its home network server and roaming in a visited network server can only reach its home network server if the two network servers are registered under the same distribution server or registered under two different distribution servers having a connection between them.

- Database Service: after each registration process, each distribution server stores in its database the NetworkID of the newly registered network server mapped to its IP address, or the collaborating distribution server mapped to its IP address. In this way, the distribution server builds a database of distribution and network servers registered with their IP addresses. This database is mainly used by the message distribution service.
- Message Distribution Service: is the service listening to incoming messages that can come from a network server or distribution server. In all cases, the distribution server must read the destination NetworkID. If the message is sent by a network server, the distribution server must check if the destination network server is accessible, so it queries the database service. If the network server is accessible directly, it extracts the network server IP and forwards the message. If the network server is accessible by another distribution server, it extracts the distribution server IP and forwards the message, otherwise it must reject it. If the message is sent from another distribution server, the current distribution server knows that it has a direct connection to the destination, so it checks and if the network server is still registered, it extracts its IP address and forwards the message. Otherwise, the message is rejected.
- Information exchange service: this service is activated if the distribution server has active collaborator distribution servers. In this case, each distribution server must periodically send an update message indicating which network server is still reachable through it, or which network server is no longer reachable. This message is sent periodically within a predefined period or conditionally depending on a certain condition that triggers the information exchange service process.

We note that this solution is based on a distributed system architecture. It has the same advantages of the first solution. Nevertheless, it bypasses many drawbacks encountered in the first solution. This solution is free of charge because it is not based on the blockchain, except in the case where the distribution server is operated by an operator wishing to provide

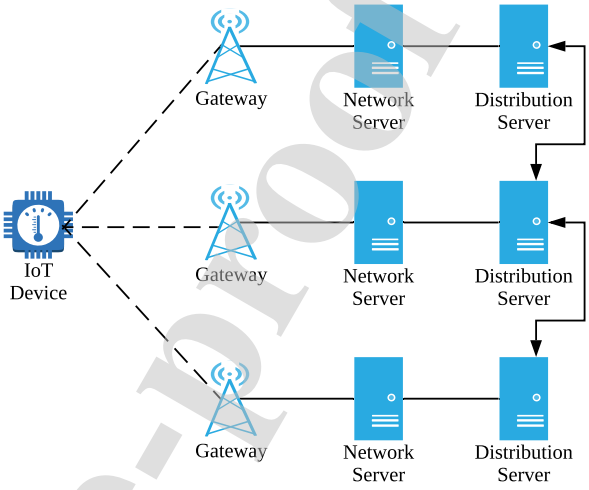


Figure 6: Distribution servers based solution.

paid services. In addition, this solution is not vulnerable to "51% attack", but on the other hand, other security issues can be found as described in section 6.

3. Mobility Management with Session Continuity during Handover in LPWAN

This solution is proposed by Ayoub *et al.* [45, 46]. The authors propose a framework to manage end device mobility between different network operators having the same technology, giving a special focus on LoRaWAN technology. The solution is based on a protocol derived from the Static Context Header Compression (SCHC) protocol [47] called Mobile Static Context Header Compression (MSCHC) and the use of Mobile IPv6 (MIPv6) protocol to facilitate the routing when moving between networks.

SCHC [48] is a protocol for IPv6 header compression based on a context stored in the end device and in the network. This context contains several rules where each rule has its unique rule identifier. Each rule contains essentially a list of IPv6 header fields with a target value, matching operator and compression/decompression action.

The compression and decompression procedures

Ext. Type = 16	Length	Sequence Number	
Registration Lifetime		Flags	Reserved
Care-of-Adress 1			
Care-of-Adress 2			
Care-of-Adress i			
Care-of-Adress N			

Figure 7: Frame sent by the gateway.

rely on the saved context. To find the best matching rule between the rules contained in the context, the procedures iterate through these rules and compare the current packet header fields to the target value according to the matching operator. The rule identifier of the best matching rule is sent instead of the entire header with the residues of the fields arising from the compression action. The context is static, which means that it is not periodically updated considering that the packet header does not change frequently as the device is still in the same network.

On the other hand, SCHC does not take into consideration the mobility of end device, which leads to the change of the used context. Thus, the authors propose to have a context that can be changed dynamically when the device moves between networks. Also, an optimization of SCHC is proposed to separate the rules in the context according to the application, transport, network and extension layer fields, which lead to more flexible uses of context and saving memory.

Furthermore, to make the IPv6 address assignment easier after entering coverage of a new network, the LoRaWAN gateway is supposed to send periodically a frame containing a list of care-of-addresses as shown in figure 7, of which the device can take one of them to communicate with the new network.

An optimization is proposed on the existing LoRaWAN roaming procedure to avoid triangular routing where any packet sent to the visited network server should be routed to the home network server before sending it to its final destination. For that, to reduce the transmission time and save network bandwidth, the binding update mechanism existing in MIPv6 is used to make direct routing between the end device and the corresponding node avoiding triangular routing.

5 Mobility Related Security Issues

In this section, we focus on security issues related to mobility causing various vulnerabilities for the network and communicating entities. The impacts of each issue in conformity with security requirements highlighted in section 2 are summarized in table 2.

5.1 Device Reauthentication

Authentication is the ability of the entities to continuously identify each other. Thus, entities should be able to identify each other before, during and when terminating a session. Hence, a mobility management process should ensure the secure management of device identities during end devices movement between different networks. In a typical scenario, an end device establishing a connection with a peer, moves from its home network towards a visited network and desires to resume the established session. For that, an identity verification mechanism should be supported by the mobility management process to verify that any message sent to the visited network is actually sent by the end device and any attempt by an attacker to steal an end device identity should be detected and prevented.

5.2 Error Message Attack

A mobility management process is a sequence of actions and operations executed by the involved entities where signaling messages can be used to control the progress of the communication. This process may fail or be interrupted before completion for many reasons, such as battery death, connection loss, etc. To ensure secure communication, the process must address all possible failures. To prove how a failure can be a source of threat, consider the following example. An end device moving out of its home network coverage towards another network coverage will trigger

the mobility management process. Suppose that the adopted process registers the end device with the visited network before reaching its coverage area. Since the process is triggered, the end device is registered now with the visited network, but for some reason, and before the process is completely terminated, the process is interrupted. If a signaling message indicating that the process is interrupted and any change must be reverted is not sent to the visited network to revoke the newly registered end device, an attacker can hijack the session that should be established between the visited network and the end device.

5.3 False Handover Request

A mobility management process is triggered under certain conditions. Suppose that the process is triggered when the received signal power drops below a certain threshold. This condition can be ill-used to trigger the process and generate a false handover request. For example, a malicious end device can move towards the boundary of its home network coverage, thus the received signal power decreases until reaching the threshold value which will trigger the process to start, then immediately, the end device will move back towards the coverage of its home network again, which lead to a false handover request. The problem caused seems insignificant if only one device is involved. But assume that a large number of end devices get involved and behave in such a way. As a result, a large number of false handover requests should be handled by the mobility management process. Thus, if a server undertakes the requests processing, this may cause performance degradation or even a deny of service if the processing power of the server is not appropriately estimated.

5.4 Spoofing Signaling Message

A signaling message holds commands to control the communication or the session flow between the entities. Various signaling protocols exist and each has its tailored signaling messages. The role of these messages is the establishment or termination of a session, update connection parameters, exposing a device state, etc. A mobility management process uses signaling messages to control the communication in the network. Messages should be exchanged securely to avoid any message alteration or spoofing. By way of illustration, assume the used mobility management process uses a signaling message that announces the end of a session between the end device with its home network. The message sender should sign it and the receiver should be able to verify the sender identity. If an attacker succeeds in spoofing this message, it can end an established session which, for example, must not be terminated. Another example for message spoofing, assume the mobility management process uses a signaling message that assigns a new identity to a mobile end device, if an attacker succeeds in spoofing this message, he can assign his identity as the new end device identity and take the control over end device session.

5.5 Address Squatting

Address squatting is preventing an end device from getting its genuine address. The address refers here to the link layer identity or the network layer address. This issue occurs when the mobility management process pre-assigns addresses for end device based on a known or predictable algorithm. Suppose that an end device moving from its home towards a visited network, the latter can identify it based on the assigned address, which cannot be given to another end device. If an attacker predicts the address generation algorithm, it claims the ownership of any valid address that should be given to another end device, and any message sent to the end device will be routed to the attacker. Thus, an end device moving towards a visited network will fail to establish a connection using its address that was stolen by the attacker. For that, it is necessary to adopt an algorithm generating addresses in unpredictable ways and supporting mechanisms protecting reactively counter address squatting.

5.6 Address Spoofing

The same scenario shown in the previous attack leads to address spoofing attack which can be seen as an active state of address squatting. The difference here

is that the attacker does not only steal the address but sends messages to other nodes that appear to come from the genuine node. To prevent such attacks, the mobility management process should not rely on the basic implementation of protocols at the link and network layers, and a suitable mechanism should be used to manage addresses and identities of end devices during mobility.

5.7 Old Address Control

Following an end device switching to a visited network, it will be assigned a new identity for the link layer and a new address for the network layer, the obsolete identity and address assigned in the home network will be released. The problem arises if the obsolete identity and address are released in a way that makes it possible for an attacker to resume the session that was established with the home network. Therefore, after completing the mobility scenario, any old session that will not be used in the future should be securely terminated.

5.8 Context Alteration

Several mobility management processes make use of context which is a sort of trace maintaining information about the end device and used to resume a session after moving from the home network to another one. The matter is how to maintain the integrity of this context while it is stored, updated or exchanged. As an example, suppose that the context contains a destination address of every message sent by the context owner. Thus, in case an attacker succeeds to change the destination address in this context, the messages will be forwarded to another destination and blocked for the intended destination. If the attacker alters a considerable number of contexts, it causes the node to be flooded with a large number of spam messages and causes at advanced levels a denial of service for that node.

	Authenticity	Confidentiality	Integrity	Availability
Device Reauthentication	✗			
Error Message Attack	✗	✗		
False Handover Request				✗
Spoofing Signaling Messages	✗		✗	
Address Squatting				✗
Address Spoofing	✗	✗		
Old Address Control	✗			
Context Alteration			✗	✗

Table 2: Impact of Mobility Related Security Issues

6 Security Evaluation

In this section, we evaluate the mobility solutions presented in section 4 according to mobility related security issues shown in section 5.

6.1 Blockchain based solution for roaming in LoRaWAN security issues

6.1.1 Device Reauthentication

The reauthentication procedure relies on the smart contract storing the array mapping JoinEUI to the corresponding home network server address. Tentatively, the solution is not susceptible to such threat, but as discussed before, the blockchain is susceptible to "51% attack", thus, if an attacker takes control over the blockchain, he can append erroneous record by mapping JoinEUI to wrong home network server and vice versa. Therefore, when a visited network server queries the smart contract for a certain JoinEUI, the returned home network server address could be faulty, and the rest of the join procedure will lead to an authentication with a faulty network

server.

6.1.2 Error Message Attack

We can perceive that process failure is well handled and this solution is not susceptible to such attack. For example, when a home network server tries to attach an already existing JoinEUI, an error message is produced by the smart contract indicating that the JoinEUI already exists in the array with another server address and duplication is hindered.

6.1.3 False Handover Request

This solution is vulnerable to false handover requests that can be sent by malicious end devices outside the coverage of their home network servers. The affected entities are the forwarding and the home network servers which will execute the entire roaming procedure without any check on messages sent by the end device. The malicious end device can still perform this harmful behavior as there are not packet filtering techniques accompanied with the roaming procedure.

6.1.4 Spoofing Signaling Message

Signaling messages used in this solution are similar to those used in LoRaWAN join procedure, as join request, join accept, home network server lookup, etc. For that, this solution inherits the security strength of LoRaWAN message exchanges which is not secure against this type of attack under certain conditions [49].

6.1.5 Address Squatting

Is prevented because the mapping between the JoinEUI and the appropriate home network server address is ensured by the smart contract which cannot be altered as the blockchain ledger is immutable, thus, an attacker cannot add a record mapping a JoinEUI with a faulty network address unless he does not possess 51% of the network processing power. Furthermore, the address assignment is based on LoRaWAN protocol where it is generated by the home network server and sent encrypted to the end device thus an attacker cannot predict this address in order to block it.

6.1.6 Address Spoofing

The same reasons preventing address squatting impede address spoofing in this solution. The device address cannot be spoofed since the home network server sends it encrypted to the end device, and messages sent by this end device are encrypted using a network session key ensuring confidentiality and while data integrity is ensured by the message integrity check.

6.1.7 Old Address Control

An attacker cannot take control over an abandoned address, as it should have the network session key of the previous session established between the abandoned device and the network server to send a message, otherwise, the network server will fail to decrypt the message and will drop it.

6.1.8 Context Alteration

Since this solution does not use any context to manage roaming, this solution will not suffer from such problem.

6.2 Distribution servers based solution for roaming in LoRaWAN security issues

6.2.1 Device Reauthentication

The authentication mechanism for end devices when moving between two networks in this solution is the same as the LoRaWAN v1.0 mechanism which is considered not secure [50].

6.2.2 Error Message Attack

By examining the solution implementation, we observe that the missteps are treated securely so that any interruption or failure during the execution of the procedure causes an error message. For example, if the address corresponding to a NetworkID where the

packet has to be forwarded is not found, the distribution server issues an error message and then drops the packet.

6.2.3 False Handover Request

The mobility management process in this solution is susceptible to this type of attack as it treats all the received packets, and for every received packet, the distribution server extracts the NetworkID and strives to get the corresponding address. If an end device sends packets with false NetworkID, each packet will be processed and dropped after that, without a tendency to block such corrupted type of packets which will lead to a degradation in the network performance. This impact becomes considerable as the number of malicious devices increases.

6.2.4 Spoofing Signaling Message

Very high risk is due to the threat of this solution to this type of attack. Signaling messages are sent in clear text without encryption. Moreover, there is neither an authentication mechanism to verify the sender identity nor an integrity check to ensure that the data are not tempered. The primary usage of signaling messages in this solution is to register or revoke a network server or another distribution server. An attacker exploiting this vulnerability can take control of the entire network, by adding and removing collaborating distribution server in a dangerous and futile way.

6.2.5 Address Squatting

Since any registration message is processed without examining the message sender, an attacker can send a registration request containing a NetworkID of a victim network i.e. the network that the attacker wants to squat his address. Therefore, the distribution server will insert in the database an entry containing the NetworkID with the attacker address. Thus, if the victim network tries to register with his correct address, it fails because the NetworkID was registered with the attacker address which make this solution vulnerable to address squatting.

6.2.6 Address Spoofing

Address spoofing is done in the same way as address squatting. The difference is that the attacker sends packets to the distribution server which considers them coming from the spoofed network.

6.2.7 Old Address Control

This solution is vulnerable to this attack. Suppose that a network server stops working and releases its address. If an attacker succeeds in obtaining the released address, it registers using the old network server NetworkID and therefore transmits messages to the distribution server as it stands as the network server. This attack leads to the same results of address spoofing, but in this case, the genuine network server address is mapped to the NetworkID and appears to the distribution server that the network server becomes active again.

6.2.8 Context Alteration

This solution does not use contexts to manage roaming in the network, thus, this solution does not experience such vulnerability.

6.3 Mobility Management with Session Continuity during Handover in LPWAN security issues

6.3.1 Device Reauthentication

The proposed solution relies on a frame that is periodically broadcasted by network gateways containing a list of care-of-addresses, where the end device claims one of these addresses as it is care-of-address. A reauthentication threat occurs if an attacker sends a binding update message mapping a faulty address, instead of the care-of-address, with the home address of the device. Consider the scenario in figure 8. The device is in its home network with link layer identity ID1, and network layer address IP1. The device moves towards the visited network broadcasting the frame, thus the device gets a care-of-address IP2 from the frame as its new network layer address, and a new link layer identity ID2 is assigned to it after joining

the network. An attacker can also join the network and get IP3 as its network layer address and a link layer identity ID3. The threat appears if the attacker sends a binding update message mapping IP3 instead of IP2 to IP1. It is clear that no authentication process is accomplished to check the link layer identity of the device sending the binding update message in the visited network since there is no collaboration and no identity management process executed before performing the binding update. Thus, this solution is vulnerable to such type of attack.

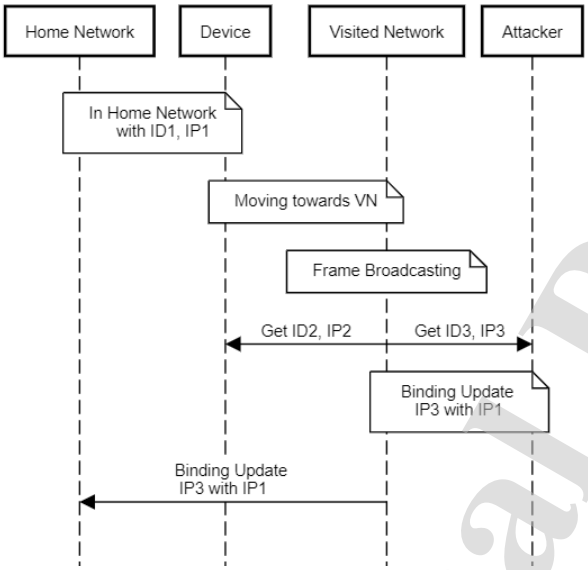


Figure 8: Device Reauthentication.

6.3.2 Error Message Attack

This solution does not tolerate any problem due to exchanged messages since no tailored signaling messages are exchanged, neither between the device and the network part nor between the home and the visited network. The only exchanged message is the binding update message sent from the device to the home network through the visited network which is a MIPv6 protocol message, and any error produced is managed by the protocol itself. As indicated above, special attention should be given to identity verification when communicating with the visited network in order to achieve a secure binding update procedure.

6.3.3 False Handover Request

After investigating [45], the list of care-of-addresses can be received by an attacker, who in his turn can assign these addresses to himself or to the devices under his control and send binding update messages to the visited network without any verification on the message sources that are sent from the same device, namely the attacker. To clarify this, consider the scenario in figure 9, the attacker devices were in their home network with their IPv6 addresses (HoA1, HoAi, HoAn). The devices move towards the visited network, and listen for frames broadcasted by the gateways of the visited network, each device will therefore request a care-of-address from the list (CoA1, CoAi, CoAn) and will send a binding update message to the visited network reaching the home network. If the number of attacker devices is large, this can cause flooding of network servers resulting in a degradation in provided QoS and even a denial of service if the server has limited processing capacity.

6.3.4 Spoofing Signaling Message

This solution is protected against spoofing signaling message, as the only one is the binding update, which, if an attacker tries to spoof it, he should use the network and link layer addresses of the target device. For the link layer address, LoRaWAN technology manages addresses in a manner to prevent two devices from having the same address, which prevents the attacker from spoofing the device identity, thus, for the network layer address, he cannot have the same address of the device also as IPv6 protocol prevents address duplication, and a binding message update cannot be sent by the attacker.

6.3.5 Address Squatting

This solution is vulnerable to address squatting because the list of care addresses is sent previously in the frame, thus an attacker can assign to himself all the addresses in the frame preventing new devices

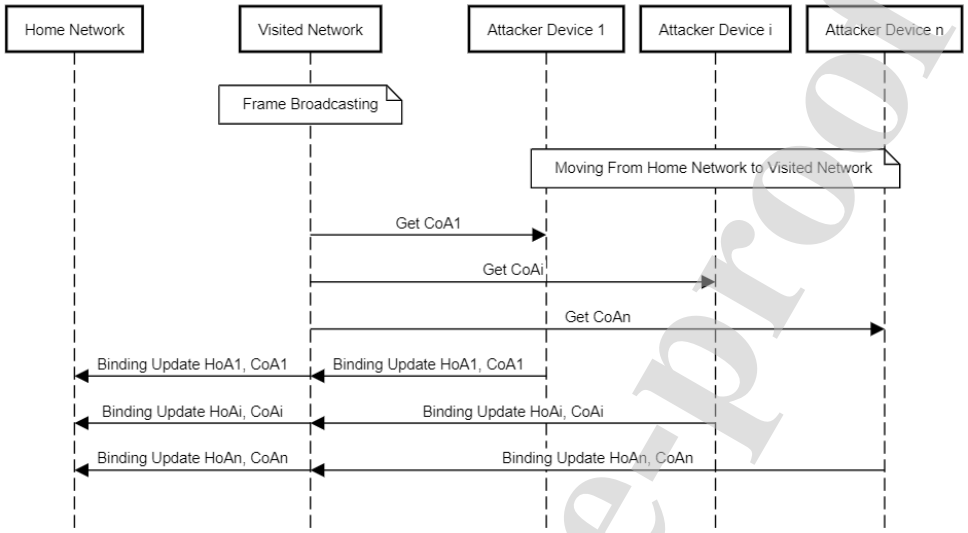


Figure 9: False Handover Request.

from obtaining addresses. For example, suppose a visited network broadcasting its frames, and an attacker mastering several devices exceeding the number of addresses in the frame. To launch the attack, each device gets an address from the list. Hence, a new device coming from its home network and receiving the frame and trying to get an address is blocked by the IPv6 protocol preventing address duplication. Thus the device cannot begin a session with the visited network causing address squatting.

6.3.6 Address Spoofing

This solution is not vulnerable to address spoofing. We can distinguish between two addressing modes, the first in the link layer, the second in the network layer. Regarding the link layer, addressing is managed by the LoRaWAN technology, thus, any try to steal or spoof the device address is detected by LoRaWAN protocol, and therefore there is no need to handle link layer addressing. Concerning network layer addressing, the used protocol is Mobile IPv6, which has a special process for address duplication detection and prevention.

6.3.7 Old Address Control

An old address control does not pose a threat to this solution. If we consider the address at the link layer, LoRaWAN technology manages addresses in a manner preventing two devices to have the same address, by generating the address and the key used for data encryption (between the network server and the device) from the device unique identifier at the start of the communication. At the network layer, old address control does not cause a problem also, as a new device gets the same address of a device leaving the network, it will start a new session with the visited network server without any impact on the network.

6.3.8 Context Alteration

The solution employs MSCHC that uses a context to compress and decompress the IPv6 packet header. This context is stored in the device and in the network, if an attacker successes to change the context content, he can change, for example, the destination of the packet, the quality of service that should be provided to the packet, or any other field in the IPv6 header.

6.4 Comparison and Open Challenges

The table 3 below summarizes the mobility related security issues and provides a comparison between the mobility management solutions presented in section 4.

When designing a mobility solution, several challenges are encountered, especially when adding security countermeasures to prevent the already mentioned security issues. The first challenge is the **mobility time**, which is the time needed to complete the mobility management process, this time consists of the pre-handoff time and the handoff time. The pre-handoff time is the time needed to perform any process or action before the device launches the handoff process. The handoff process is the process where the device releases its connection with the old network and establishes a connection with the new network. Thus, the time needed to perform the handoff process is the handoff time. Pre-handoff time does not have a direct impact on the device QoS, but the handoff time should be taken into consideration and minimized to achieve a seamless handoff procedure especially for applications that are not time tolerant. Regarding the proposed solutions, we can note that solution 1 relies on blockchain. A blockchain transaction containing the mapping of the JoinEUI with the address of the home network server requires about 14 seconds in the Ethereum to be validated and secured. The transaction validation time is considered as a pre-handoff time if sent early by the home network server, otherwise, a transaction sent late could have a serious impact on the mobility process which may fail in this case. Solution 2 relying on distribution servers has an acceptable handoff time and solution 3 relying on MSCHC compression algorithm have approximately zero handoff time as it takes a proactive approach to manage mobility which makes this solution more adapted. We know that LPWAN technologies are not designed for real time applications, but the time of handoff should stay under a certain threshold whatever is the type of the used application.

Another challenge is reducing the **number of signaling messages** exchanged between the different parties involved in the mobility management process, as more signaling messages means more transmissions, receptions and processing of these exchanged messages. Also we should take into account that the number of allowed exchanged messages is limited in certain LPWAN technologies as shown in section 1. Also, **route optimization** is a challenge that can be seen as an optimization of the overall solution. Route optimization is a way to establish a direct path between the end device and the correspondent node through the visited network server without passing through its home network server, this reduces the time needed to route a packet from the source to the destination at the cost of other parameters, more bandwidth or payload length, according to the adopted approach. We can notice that route optimization is implemented in solution 3 only, whereas solutions 1 and 2 does not include such optimization.

The challenges of mobile IoT become difficult as application, network and security constraints tighten. For that, special solutions must be designed for each constraint in order to achieve a complete framework for managing mobility in a secure and seamless manner.

	Solution 1	**Solution 2**	**Solution 3**
Device Reauthentication	✗	✓	✓
Error Message Attack	✗	✗	✗
Fake Handover Request	✓	✓	✓
Spoofing Signaling Messages	✓	✓	✗
Address Squatting	✗	✓	✓
Address Spoofing	✗	✓	✗
Old Address Control	✗	✓	✗
Context Alteration	✗	✗	✓

✓ : Vulnerable ✗ : Not Vulnerable

Table 3: Comparison of solutions according to security issues

7 Conclusion

In this paper, we investigated the mobility related security issues in LPWAN networks. We started by presenting the typical IP-based protocol stack for IoT as well as the security requirements. Then we focused on LPWAN networks and we reviewed the existing mobility solutions. Then we shed light on mobility related security issues by checking the attacks that can be performed in case of mobility for each mobility management solution. We can conclude that different attacks could be performed when using the above mobility solutions which may cause damage. Thus, there are rooms for improvement of such solutions and the development of new secure mobility management solutions.

References

[1] B. Vejlgaard, M. Lauridsen, H. Nguyen, I. Z. Kovács, P. Mogensen, and M. Sorensen, "Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot," in *2017 IEEE 85th vehicular technology conference (VTC Spring)*, IEEE, 2017, pp. 1–5.

[2] W. Ayoub, A. E. Samhat, M. Mroue, H. Joumaa, F. Nouvel, and J.-C. Prévotet, "Technology selection for iot-based smart transportation systems," in *Vehicular Ad-hoc Networks for Smart Cities*, Springer, 2020, pp. 19–29.

[3] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.

[4] N. Sornin and A. Yegin, "Lorawan backend interfaces 1.0 specification," *Lora Alliance Standard Specification*, vol. 11, 2017.

[5] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3gpp narrowband internet of things," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 117–123, 2017.

[6] J. C. Zuniga and B. Ponsard, "Sigfox system description," *LPWAN@ IETF97, Nov. 14th*, vol. 25, 2016.

[7] D. A. M. Specification, *Dash7 alliance std*, 2013.

[8] W. Ayoub, F. Nouvel, A. E. Samhat, J.-C. Prevotet, and M. Mroue, "Overview and measurement of mobility in dash7," in *2018 25th International Conference on Telecommunications (ICT)*, IEEE, 2018, pp. 532–536.

[9] X. P. Costa, R. Schmitz, H. Hartenstein, and M. Liebsch, "A mipv6, fmipv6 and hmipv6 handover latency study: Analytical approach," in *IST Mobile & Wireless Telecommunications Summit*, Citeseer, vol. 6, 2002, pp. 100–105.

[10] E. Ivov and T. Noel, "An experimental performance evaluation of the ietf fmipv6 protocol over ieee 802.11 wlans," in *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.*, IEEE, vol. 1, 2006, pp. 568–574.

[11] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (nemo) basic support protocol," 2005.

[12] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, *et al.*, "Proxy mobile ipv6," 2008.

[13] G. Ferré and E. Simon, "An introduction to sigfox and lora phy and mac layers," 2018.

[14] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[15] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[16] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[17] S. Cirani, G. Ferrari, M. Picone, and L. Veltri, *Internet of Things: Architectures, Protocols and Standards*. John Wiley & Sons, 2018.

[18] Z. Shelby, K. Hartke, C. Bormann, B. Frank, *et al.*, "The constrained application protocol (coap)," 2014.

[19] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.

[20] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of things: Survey and open issues of mqtt protocol," in *2017 International Conference on Engineering & MIS (ICEMIS)*, IEEE, 2017, pp. 1–6.

[21] P. Saint-Andre, K. Smith, R. Tronçon, and R. Troncon, *XMPP: the definitive guide.* " O'Reilly Media, Inc.", 2009.

[22] M. Laine, "Restful web services for the internet of things," *Online]. Saatavilla: http://media. tkk. fi/webservices/personnel/markku_laine/restful _web_services_for _the_internet_of_things. pdf*, 2012.

[23] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Computing*, vol. 10, no. 6, pp. 87–89, 2006.

[24] W. Shang, Y. Yu, R. Droms, and L. Zhang, "Challenges in iot networking via tcp/ip architecture," *Technical Report NDN-0038. NDN Project*, 2016.

[25] R. A. Yaiz and O. Öztürk, "Mobility in ipv6," *MSc, University of Twente, Neitherlands*, 2006.

[26] J. Hui, P. Thubert, *et al.*, "Compression format for ipv6 datagrams over ieee 802.15. 4-based networks," 2011.

[27] W. Ayoub, M. Mroue, F. Nouvel, A. E. Samhat, and J.-C. Prévotet, "Towards ip over lpwans technologies: Lorawan, dash7, nb-iot," in *2018 sixth international conference on digital information, networking, and wireless communications (dinwc)*, IEEE, 2018, pp. 43–47.

[28] W. Ayoub, F. Nouvel, S. Hmede, A. Samhat, M. Mroue, and J.-C. Prévotet, "Implementation of schc in ns-3 simulator and comparison with 6lowpan," 2019.

[29] A. Agarwal and A. Agarwal, "The security risks associated with cloud computing," *International Journal of Computer Applications in Engineering Sciences*, vol. 1, pp. 257–259, 2011.

[30] L. Alliance, "Lorawan™ 1.1 specification," *LoRa Alliance*, vol. 11, pp. 2018–04, 2017.

[31] L. Vangelista and M. Centenaro, "Worldwide connectivity for the internet of things through lorawan," *Future Internet*, vol. 11, no. 3, p. 57, 2019.

[32] N. Blenn and F. Kuipers, "Lorawan in the wild: Measurements from the things network," *arXiv preprint arXiv:1706.03086*, 2017.

[33] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1561–1581, 2018.

[34] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the energy performance of lorawan," *Sensors*, vol. 17, no. 10, p. 2364, 2017.

[35] G. Yang, D. S. Wong, and X. Deng, "Formal security definition and efficient construction for roaming with a privacy-preserving extension.," *J. UCS*, vol. 14, no. 3, pp. 441–462, 2008.

[36] S. Chacko and M. D. Job, "Security mechanisms and vulnerabilities in lpwan," in *Iop Conference Series: Materials Science and Engineering*, IOP Publishing, vol. 396, 2018, p. 012 027.

[37] G. Association *et al.*, "Nb-iot deployment guide to basic feature set requirements," *En ligne]. Disponible sur: https://www. gsma. com/iot/wp-content/uploads/2018/04/NB-IoT_Deployment_Guide_v2_5Apr2018. pdf.[Consulté le: 10-mai-2019]*, 2017.

[38] J.-G. Remy and C. Letamendia, "Lte standards and architecture," *LTE standards*, pp. 1–112, 2014.

[39] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J.-P. Koskinen, "Overview of narrowband iot in lte rel-13," in *2016 IEEE conference on standards for communications and networking (CSCN)*, IEEE, 2016, pp. 1–7.

[40] C. Perkins *et al.*, *Ip mobility support*, 1996.

[41] A. Durand, P. Gremaud, and J. Pasquier, "Decentralized lpwan infrastructure using blockchain and digital signatures," *Concurrency and Computation: Practice and Experience*, e5352, 2019.

[42] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[43] M. Bastiaan, "Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin," in *Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin. pdf*, 2015.

[44] J. Lamberg-Liszkay and T. Lisauskas, *An alternative roaming model inlorawan*, 2018.

[45] W. Ayoub, F. Nouvel, A. E. Samhat, M. Mroue, and J. Prévotet, "Mobility management with session continuity during handover in lpwan," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[46] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, H. Jradi, and J.-C. Prévotet, "Media independent solution for mobility management in heterogeneous lpwan technologies," *Computer Networks*, vol. 182, p. 107 423, 2020.

[47] C. Minaburo and L. Toutain, *Lpwan static context header compression (schc) and fragmentation for ipv6 and udp draft-ietf-lpwanipv6-static-context-hc-17*, 2018.

[48] W. Ayoub, M. Mroue, A. E. Samhat, F. Nouvel, and J.-C. Prévotet, "Schc-based solution for roaming in lorawan," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, Springer, 2019, pp. 162–172.

[49] X. Yang, "Lorawan: Vulnerability analysis and practical exploitation," *Delft University of Technology. Master of Science*, 2017.

[50] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of lorawan," *Computer Networks*, vol. 148, pp. 328–339, 2019.

Hassan Jradi

Hassan Jradi received the Bachelor of Engineering in "Telecommunications" from the Lebanese University in 2019, the Master of Engineering in "Telecommunications, Network and Security" from the University Saint Joseph of Beirut in 2019. He is currently a Ph.D. student at the Lebanese University in the Centre de Recherche Scientifique en Ingénierie (CRSI), Lebanon, and the Institut National des Sciences Appliquées (INSA) de Rennes in the Institut d'Électronique et des Technologies du numéRique (IERT), France. His research interests are the IoT networks, security and mobility in IoT networks, and the Low Power Wide Area Networks (LPWANs).

Abed Ellatif Samhat

Abed Ellatif Samhat received the engineering diploma in electrical and electronics from the Lebanese University, Beirut, Lebanon, in 2000, and the master degree and the Ph.D. degree in computer science from Pierre et Marie Curie University, Paris, France, in 2001 and 2004, respectively. From 2005 to 2008, he was a Research Engineer with France Telecom Group, Orange Labs–Paris, where he was involved in several national and European projects, including ambient networks and Gandalf. In 2009, he joined Lebanese University, where he is currently a Professor with the Faculty of Engineering. His areas of interest include heterogeneous wireless networks, cross-layer design, access selection, mobility management and security.

Fabienne Nouvel

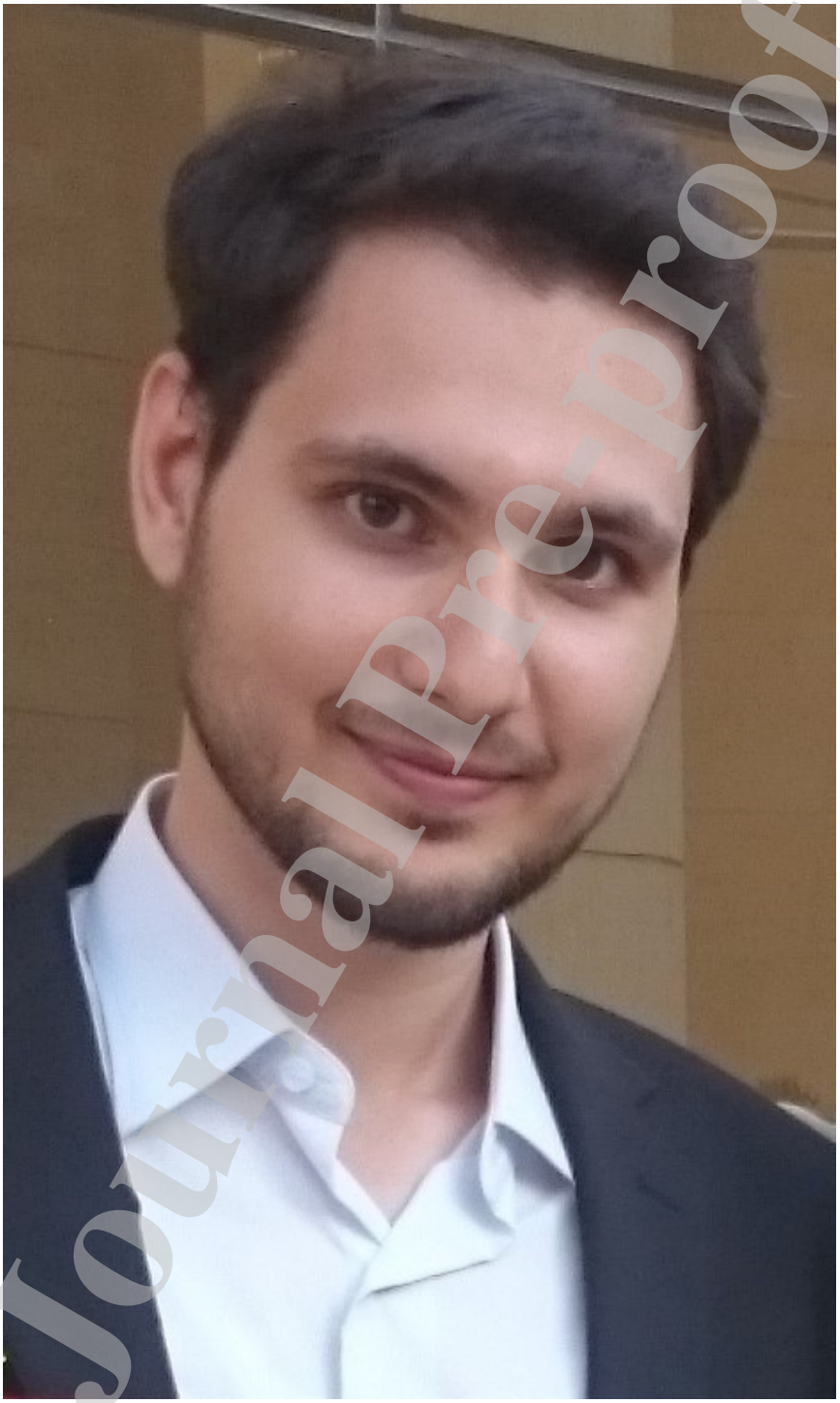
Fabienne Nouvel received the engineering diploma in electronics in 1985 and the Ph.D. degree in 1994. In 1995, she joined the Institute of Electronic and Telecommunication of Rennes, Rennes, France. She is currently a Professor of digital electronics and networks with the Department of Electronic and Network, Engineer School INSA, Rennes. Her research is focused on embedded communication systems, more particularly the power line communications in vehicles, multi-carriers, MIMO, and the implementation of such applications on digital systems. She is currently researching on applications around IoT, in a context of mobility, security integrating the dynamic reconfiguration of modems, and electrical vehicles in order to optimize the consumption.

Mohamad Mroue

Mohamad Mroue received the Engineering Diploma in Signal Processing and Telecommunications and the Master's degree in Electronics from the University of Rennes 1 in 2005, and the Ph.D. in Electronics from INSA Rennes in 2009. He was with Mitsubishi Electric Research and Development Centre Europe, where he researched on the implementation of Ultra Wide Band systems for High Data Rate applications. In 2009, he joined Supélec, where he worked as a post-doctoral researcher on the PAPR problem for Digital Video Broadcasting systems. In 2010, he moved to Lebanon, where he worked as a faculty member at Saint Joseph University, Notre Dame University – Louaize, and Antonine University. In 2014, he joined the Lebanese University as an Assistant Professor, where he has been an Associate Professor with the Faculty of Engineering since 2018. His current research activities are focused on the study and implementation of wireless communication systems.

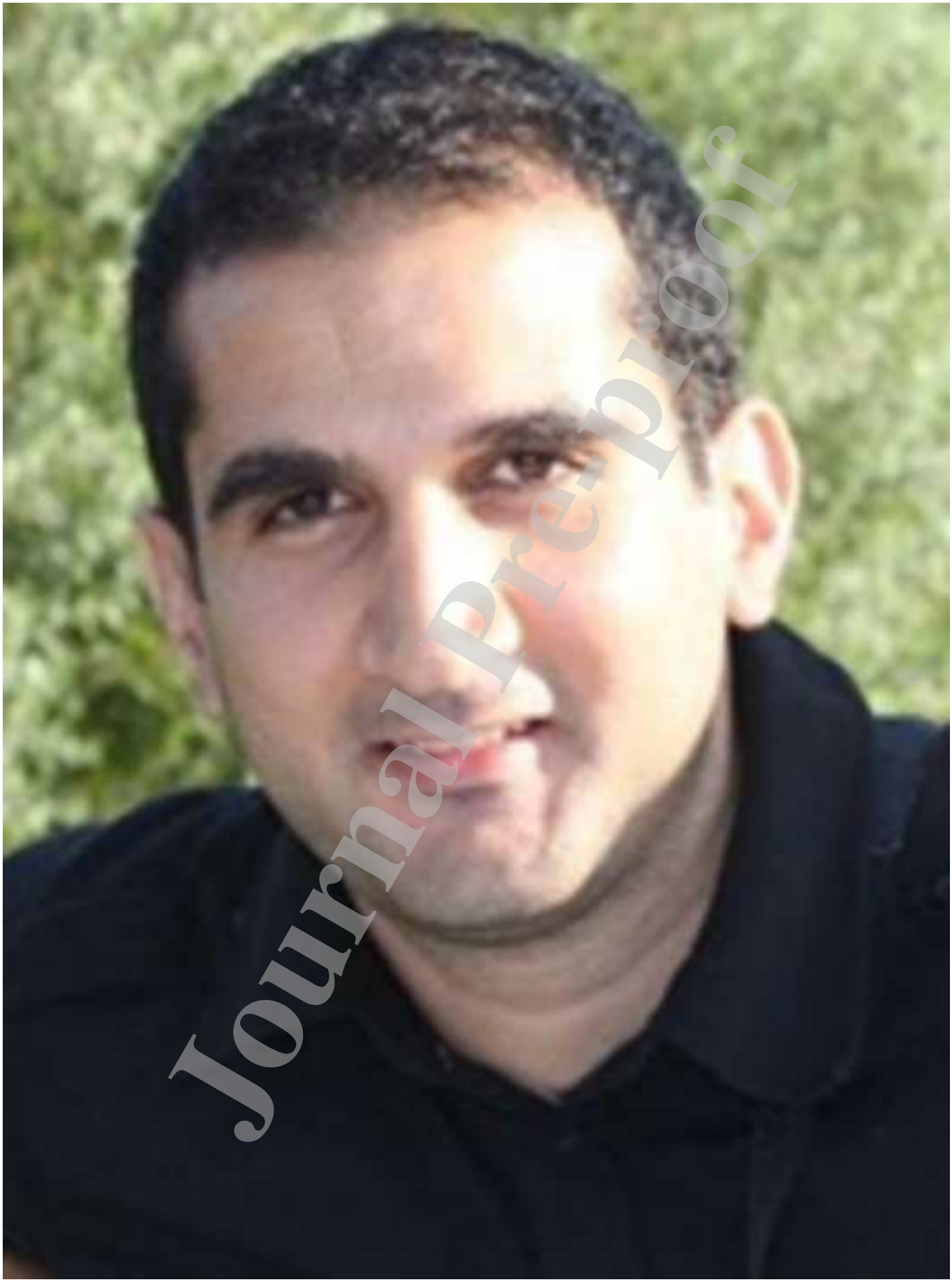
Jean-Christophe Prévotet

Jean-Christophe Prévotet received the Ph.D. degree from Pierre et Marie Curie University, Paris, France, in 2003. He is currently an Associate Professor with IETR/INSA de Rennes, Rennes, France. His major interests are embedded and reconfigurable systems and real-time systems in general. His applicative subjects deal with communication systems and the way to optimize their architecture onto a real platform. He is also deeply involved in the real-time management of these communication platforms under the supervision of an embedded operating system.



Fabienne Nouvel Ph nne

Nouvel.jpg



Prevotet.jpg

Conflict of Interest and Authorship Conformation Form

Please check the following as appropriate:

- All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.
- This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.
- The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript
- The following authors have affiliations with organizations with direct or indirect financial interest in the subject matter discussed in the manuscript:

Author's name	Affiliation
Hassan Jradi	Lebanese University, CRSI, INSA Rennes, IETR
Abed Ellatif Samhat	Lebanese University, CRSI
Fabienne Nouvel	INSA Rennes, IETR
Mohamad Mroue	Lebanese University, CRSI
Jean-Christophe Prévotet	INSA Rennes, IETR